Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

	ADPPA	CCPA/CPRA	Compare
Covered Entities	• Any person or entity (excluding individuals acting in a non-commercial context) that (1) alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and (2) is covered under the FTC Act, is a common carrier, or is a non-profit organization. • Places some extra requirements on "large data holders" and gives some exemptions and other special treatment to small businesses, including exemption from the private right of action. • Carves out entities that provide assistance regarding missing and exploited children. • Excludes gov't service providers from the covered entity definition, but regulates them as service providers.	• Entities that: 1) have annual gross revenue in excess of $25M; or, (2) collect the personal information of >100,000 consumers; or, (3) derive 50% or more of its revenue from selling consumers' personal information. • Any third party that receives data has to make representations and operate under a contract, so even entities that do not meet the "business" definition under CCPA are still subject to certain regulations.	Roughly equivalent. ADPPA covers most entities that handle covered data and then either adds or removes requirements depending on whether an entity is a large or small business. CCPA excludes nonprofits and small businesses from its "business" definition but does impose certain rules and restrictions on third parties that handle data.
Future Amendments	• Congress has the power to amend ADPPA in the future in ways that could strengthen or weaken privacy protections. • States would not be permitted to pass future laws covered by ADPPA and not explicitly preserved in the statute.	• The CPRA ballot initiative provides that amendments to the CCPA must be in furtherance of the privacy intent of the measure, so the CA legislature cannot go below a "floor" of protections.	CA law is stronger. The CCPA/CPRA provide a protection against amendments that would weaken privacy.

Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

Data Minimization & Privacy Protections			
Data minimization	• Imposes a baseline duty on all covered entities not to unnecessarily collect or use covered data, regardless of any notice or consent. • Limits the collection, processing, and transfer of covered data unless limited to what is reasonably necessary and proportionate to provide or maintain a product or service requested by the individual, or effect an expressly permitted purpose.	• Limits the collection, use, retention, and sharing of a consumer's data to what is reasonably necessary and proportionate to achieve the purposes for which it was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.	ADPPA is stronger. ADPPA's data minimization requirements are more specific and provide more detailed restrictions. The CCPA section on use limits could be a basis for specific rules, but CPPA has not yet imposed such rules.
Heightened Protections and Sensitive Data	• Imposes stricter data minimization rules for sensitive covered data: it cannot be collected or used beyond what is strictly necessary to provide service or for expressly enumerated purposes. • Enumerated purposes include: processing necessary to provide service requested; limited internal operations, improving a product or service for which the relevant data was collected; user authentication; security, harm, and fraud prevention; to comply with legal obligations; product recalls; public interest research; and to deliver P2P communications. • Transfer of sensitive covered data to third	• Heightened protections for sensitive data only apply when such data is collected/processed for "the purpose of inferring characteristics about a consumer." • In such circumstances, a business may use sensitive data without consent as necessary to provide service, for security, for transient non-personalized first party advertising, internal operations, quality assurance, or other purposes authorized by rulemaking. • In other circumstances, businesses can use sensitive data with notice to users and the option to opt-out. • Grants CA residents the right to limit the use of their "sensitive" personal data on an	ADPPA is more protective because rather than requiring users to take action to limit the use of their sensitive data (via an opt-out link), ADPPA limits use of sensitive data by default unless strictly necessary to provide a service or for one of the specified permissible purposes. However, unlike the CCPA, the ADPPA does

	parties is prohibited without opt-in consent (with a few narrow exceptions). ● "Sensitive covered data" includes gov't identifiers, health info, financial info, biometric & genetic info, precise geolocation, private communications, login credentials, sexual behavior, race, color, ethnicity, religion, union membership, online activities over time, intimate images, and minors' data. ● FTC can designate new categories by rulemaking.	opt-out basis. ● "Sensitive personal information" includes govt. identifiers; health info; financial info; biometric and genetic data; login credentials; location info; race, religion, or union membership; communications content; and sexual behavior info. ● The CA Privacy Protection Agency can add more categories by rulemaking.	not provide an individual right to limit further processing of sensitive data.
Use and disclosure limitations and controls	● Data minimization provisions (see above) limit use and disclosure. ● Collection, use, and transfer of information identifying an individual's online activities over time and across third party websites & services is limited, cannot be used for ads ● Right to withdraw previously given consents. ● Right to opt-out of covered data transfers to third parties. ● Right to opt-out of targeted advertising. ● Requires compliance with unified opt-out mechanisms.	● Data minimization provisions (see above) limit use and disclosure but current regulations permit secondary uses with user express consent. ● Right to withdraw previously given consent. ● Users have the option to opt-out of the sale or sharing of their personal information. ● Requires compliance with unified opt-out mechanisms.	Roughly equivalent. The CCPA includes several different opt-out mechanisms whereas ADPPA more directly limits uses by default and provides a right to opt-out of both transfers to third parties and targeted advertising.
Manipulative design restrictions	● Prohibits obtaining consent in ways that are misleading or manipulative (e.g., dark patterns). ● Prohibits deceptive advertising.	● The CCPA prohibits obtaining consent through dark patterns or manipulative design. ● The proposed CCPA regulations identify	Roughly equivalent. The proposed CCPA regulations provide more specific guidance

		specific design principles for obtaining consumer consent in ways that are not manipulative. • California UDAP law prohibits deceptive advertising.	on manipulative design. The ADPPA does not provide specific rulemaking authority on manipulative design.
Take-it-or-leave-it terms and pay-for-privacy	• Covered entities may not deny, condition, or effectively condition the provision or termination of services or products to individuals by having individuals waive any privacy rights in the Act. • Does allow covered entities to offer different pricing to individuals who request their data be deleted. • Covered entities are not prevented from offering bona fide loyalty programs. • Covered entities may offer incentives to participate in market research. • Covered entities can offer different pricing or functionality if a user requests to delete their covered data.	• Businesses may not discriminate against a consumer because the consumer exercised any of the consumer's rights. • However, CCPA allows businesses to offer "financial incentives," including payments to consumers as compensation for the collection, sale, or retention of their personal information. Such incentives may not be unjust, unreasonable, coercive, or usurious in nature. • It also allows businesses to offer a different price, rate, level, or quality of goods or services if the price is "reasonably related to the value provided to the business by the consumer's data."	CA law is slightly stronger as it places guardrails on financial incentives and discounts to ensure fairness.
Transparency	• All covered entities and service providers must have privacy policies that meet a certain standard. • Large data holders must also provide short-form notices. • Entities must notify individuals affected of material changes to privacy policies & offer opportunity to withdraw consent.	• Covered businesses must provide privacy notices that meet a certain standard. • Covered businesses must notify consumers if they use data beyond the disclosed purpose. • CPPA authorized to issue regulations to ensure this notice may be easily understood by the average consumer.	Roughly equivalent.

Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

Civil Rights and Algorithmic Fairness			
Prohibits discriminatory uses of data	• Covered entities and service providers may not collect, process, or transfer covered data in a manner that discriminates on the basis of race, color, religion, national origin, sex, or disability. • Covers intentional discrimination and disparate impact. • Exempts self-testing and DEI programs.	• No relevant provisions in CCPA/CPRA. • California Unruh Civil Rights Act prohibits discrimination by businesses, but it applies only to intentional discrimination, not disparate impact.	ADPPA is more protective. *Note: All state civil rights laws are exempt from preemption under ADPPA.*
Algorithmic Impact Assessments	• Requires large data holders to conduct annual algorithmic impact assessments on algorithms that pose a consequential risk of harm and submit to the FTC. • Impact assessments must include steps taken to mitigate harms related to minors, disparate impact on basis of protected characteristics, life opportunities, etc. • Algorithmic evaluations must also occur at the design phase of an algorithm, including evaluating any training data that is used to develop the algorithm.	• Covered businesses must conduct regular risk assessments weighing the benefits of their data processing (which includes using algorithms) against risks to consumers, with the goal of not engaging in practices whose risks outweigh their benefits. • Must be submitted to CPPA. • CPPA can issue regulations governing these risk assessments.	ADPPA is slightly more protective because it requires the algorithmic impact assessments to focus on algorithmic bias and the risks from discrimination, which feeds into ADPPA's prohibition of discriminatory data uses.
Automated Decision Making Rights	• No opt-out right for automated decision making (but anti-discrimination provisions apply to automated decision making).	• CPPA can issue regulations regarding application of access and opt-out rights to automated decision making.	CA offers a right to opt-out of automated decision making that ADPPA does not. This right would not be preempted by ADPPA.

Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

Enhanced Protections for Kids & Teens			
Kids/teens protections	• Targeted advertising is expressly prohibited to individuals under 17. • Covered entities may not transfer the covered data of minors without express affirmative consent. • Establishes a Youth Privacy and Marketing Division at the FTC. • Algorithmic impact assessments must assess and mitigate harms to kids and teens. • Kids' data is protected as sensitive data.	• Kids' data cannot be sold unless parents (for kids under 13) or teens (ages 13–15) opt-in to sale.	ADPPA is more protective because it has strict data minimization requirements and use limits and prohibits targeted advertising to kids and teens.
Data Brokers			
Data Broker Registry	• Data Brokers ("Third Party Collecting Entities") must register with the FTC. • The FTC will create a national registry of data brokers so that individuals can find them and exercise their rights. • Data brokers are also covered entities subject to the rest of the Act.	• A separate California law requires data brokers to register with the state. • Data brokers are subject to CCPA opt-out and other protections.	Roughly Equivalent
Data Broker Opt-out	• Requires the FTC to establish a "Do Not Collect" mechanism where individuals may submit a single request to all registered data brokers to have their covered data deleted within 30 days.	• Data brokers are required to provide the same "Do not sell or share my information" link as other covered businesses.	ADPPA is stronger. Individuals do not know which data brokers hold their info, therefore CA link is insufficient.

Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

Data Security and Corporate Accountability			
Data Security Requirements	• Covered entities and service providers must have reasonable data security practices and procedures, based on their size, nature and scope of processing, volume and sensitivity of data, current state of the art, and cost. • Large data holders must conduct biennial audits to ensure compliance with all applicable laws and submit audit reports to the FTC upon request.	• Covered businesses must implement reasonable security procedures and practices appropriate to the nature of the personal information to protect from unauthorized or illegal access, destruction, use, modification, or disclosure. • Covered businesses must conduct cybersecurity audits.	Roughly equivalent.
Executive Responsibility	• An executive must personally certify compliance with the Act.	• No requirement that an executive must personally certify compliance with the Act.	ADPPA is more protective.
Privacy Impact Assessments	• Covered entities (except small businesses) must conduct biennial privacy impact assessments that weigh the benefits of data use against the potential adverse consequences to individual privacy. • PIAs by large data holders must be approved by the entity's privacy protection officer.	• Covered businesses must conduct regular risk assessments weighing the benefits of their data processing against risks to consumers, with the goal of not engaging in practices whose risks outweigh their benefits. • Must be submitted to CPPA. • CPPA can issue regulations governing these risk assessments. • Third parties whose data practices may pose a risk to consumers may also be required to implement PIAs.	Requirements for assessments are roughly equivalent, but CCPA stronger because assessments must be submitted to the CPPA, improving transparency.

Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

Service Providers and Third Parties			
Service Providers	• Service providers can only collect, process, and transfer data to the extent necessary and proportionate to provide service requested by covered entity. • Service providers shall not collect, process, or transfer data if they have actual knowledge the covered entity violated the Act. • Requirements for service provider contracts, including a prohibition on commingling data from multiple covered entities. • Covered entity not liable for service provider violations if, at time of transfer, they had no reason to know the service provider was likely to violate the Act. • Service providers are not liable for covered entity violations of the Act if they received covered data in compliance with the Act. • Covered entity must exercise reasonable due diligence in selection of service providers.	• Service providers may not retain, use, or disclose the information outside of the direct business relationship. • Requirements for service provider contracts, including a prohibition on commingling data from multiple businesses, or using data for purposes other than serving the business. • Service providers receiving personal data from a business must provide the same level of protection as the original business was obligated to provide under the law • Businesses not liable for service provider violations if, at time of data transfer, they did not have actual knowledge, or reason to believe, that the service provider intended to violate the Act. • Grants CPPA rulemaking authority to define the business purposes for which businesses and service providers may use consumers' personal information "consistent with consumers' expectations"	Roughly equivalent.
Third Parties	• Individuals can opt-out of covered data transfers to third parties. • Third parties cannot process sensitive covered data beyond the purpose for which opt-in consent was obtained. • Third parties cannot process non-sensitive	• Third parties may not sell or share personal information that has been sold to or shared with the third party by a business unless the consumer is given the opportunity to opt-out. • Proposed regulations require that a	Roughly equivalent. The proposed CCPA regulations would impose strict contract requirements on all third parties that process

	covered data beyond purposes disclosed in the covered entity's privacy notice as the reasons for which the covered entity transfers data to third parties. • Covered entity must exercise reasonable due diligence in deciding to transfer data to third party. • Third parties typically will also be covered entities subject to the bill's requirements.	business must have a contract with every third-party that receives data, ensuring there are no transfers to third parties that fall outside the scope of the law. • Third parties must provide the same level of protection as the original business was obligated to provide under the law • Businesses are not liable for third party violations if, at time of data transfer, they did not have actual knowledge, or reason to believe, that the third party intended to violate the Act.	personal information.
User Rights			
Right to access, correct, and delete	• Grants rights to access/correct/delete and for data portability. • Establishes exceptions and gives FTC rulemaking authority.	• Grants right to access/correct/delete/ and for data portability.	Roughly equivalent.
Accessibility			
Language Accessibility	• Entities are required to provide notices in all languages it provides service in. • FTC must also publish guidance documents in multiple languages.	• Statute grants CPPA rulemaking authority to ensure that notices required under CCPA are available in the language primarily used to interact with the consumer.	Roughly equivalent.
Disability Accessibility	• Entities required to provide notices & mechanisms in a manner that is accessible & usable by individuals with disabilities.	• CPPA has rulemaking authority to ensure that notices required under CCPA are accessible to individuals with disabilities.	Roughly equivalent.

Comparison of American Data Privacy and Protection Act vs. California Privacy Laws

Enforcement			
Government Enforcement	• New Bureau of Privacy at FTC to enforce the Act. • State AGs and state privacy agencies can also bring lawsuits. • Statute explicitly grants enforcement authority to the CPPA. • FTC can create "technical compliance programs" to guide businesses on compliance with the Act in certain areas, but it is not a safe harbor and doesn't affect burden in enforcement.	• CA Privacy Protection Agency (CPPA) enforces and issues regulations. • CPPA can get statutory civil penalties. • CPPA has a Chief Privacy Auditor who can audit businesses to ensure compliance with the law. • Violations of CCPA can also be enforced by over 60 district and city attorneys.	ADPPA has nationwide enforcement by FTC and state AGs and privacy agencies CPPA. California law cannot directly protect people outside California.
Private right of action	• Available for violations involving sensitive covered data, pay-for-privacy, transparency, individual rights, consents and opt-outs, kids' protections, data brokers, civil rights, data security, service providers, third parties. • PRA goes into effect after two years. • Persons or classes of persons may bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs. • Some procedural hurdles include limits on pre-dispute monetary demands, requirement to notify FTC and state AGs, right to cure for claims for injunctive relief. • Small businesses are exempt from PRA.	• The CCPA only provides a private right of action for data breaches.	ADPPA has a stronger private right of action because it can be used to enforce a broader range of violations. CCPA does provide statutory damages for data breach; ADPPA does not provide statutory damages. *Note: ADPPA does not preempt CCPA's data breach private right of action.*